**СИСТЕМА ЦИРКОНИЙ-С2000**

***Назначение и область использования***

Предназначена для использования в качестве системной основы для создания централизованных комплексов безопасности средних и крупных объектов, в том числе расположенных на пространственно разнесенных территориях. Обеспечивает разграничение и контроль доступа персонала внутри объекта, охрану периметров, расположенных на территории объекта зданий, сооружений, зон (помещений).

Комплекс безопасности объекта, построенный на базе системы "Цирконий-С2000", позволяет существенно улучшить эффективность охраны по предупреждению диверсий, хищений, саботажа, а также поддерживать на надлежащем уровне порядок в деятельности объекта, успешно решая важные задачи:

- повышения трудовой и технологической дисциплины;

- оперативного управления действиями персонала;

- учета использования рабочего времени;

- снижения вероятности появления чрезвычайных и аварийных ситуаций, повышение достоверности анализа причин их возникновения и эффективности работ по ликвидации последствий.

Система «Цирконий-С2000» БАЖК.425621.002-03 по БАЖК.425621.002-03 ТУ имеет Декларацию соответствия ТР ТС ЭМС и безопасность НВО ТС № RU

Д-RU.АЮ02.В.03243

***Принцип действия***

При создании централизованного комплекса безопасности на базе системы «Цирконий-С2000» охраняемый объект делится на участки по периметру и зоны по территории, зданиям, сооружениям. На каждом участке, в каждой зоне устанавливаются средства обнаружения (СО), на входе в зону и выходе из зоны – средства контроля и управления доступом. Информация о функционировании выше перечисленных технических средств передается на станционную часть системы, где она регистрируется, обрабатывается, оперативно отображается на рабочих местах операторов и заносится в память. Станционная часть системы, реализованная на основе локальной вычислительной сети, обеспечивает подачу команд управления на СО, средства управления и контроля доступом.

Для управления доступом каждому сотруднику или посетителю (далее по тексту – абоненту) выдается карта-пропуск, которая используется как один из идентификаторов личности при проходе через точки доступа. Дополнительным идентификатором может служить набираемый сотрудником личный код, при необходимости, может использоваться один из биометрических признаков (изображения кисти руки или отпечаток пальца) при подключении соответствующих устройств. По результатам идентификации принимается решение о доступе или запрете доступа в зону. Все события, хранящиеся в памяти, могут быть выведены на экран ПЭВМ для ретроспективного анализа ситуаций и на принтер в виде отчетов по любым видам сообщений.

***Состав и структура***

Система "Цирконий-С2000" является гибкой, архитектурно открытой системой с иерархическим распределением функций по компонентам нескольких уровней (рисунок 1).

Каждое автоматизированное рабочее место (АРМ) специализировано под выполнение определенных функций за счет установки соответствующего программного обеспечения и настройки связей между составными частями системы.

АРМ операторов, работающие непрерывно в круглосуточном режиме, образуют оперативный уровень управления комплекса безопасности объекта и обеспечивают, в том числе с использованием графических планов, интерфейс пользователя для управления разнообразной периферийной аппаратуры: контроллерами, СО, электромеханическими запирающими устройствами (ЭМЗУ), турникетами и т.п.

АРМ для изготовления пропусков на основе Prox-карт обеспечивает подготовку макетов пропусков, ввод персональных данных абонентов, в том числе ввод их фотографии с помощью цифрового фотоаппарата или сканера, печать пропусков и учетных карточек о выдаче пропуска.

АРМ администратора предназначен для конфигурирования системы, ведение базы данных абонентов с разрешительными данными, формирование и печать отчетов о событиях в системе по архиву сообщений.

АРМ отдела кадров осуществляет формирование отчетов о трудовой дисциплине (опоздание, отсутствие на рабочем месте, уход с работы ранее установленного времени) и ведет электронный табель учета использования рабочего времени.

Число АРМ любого вида в системе не ограничено. В системе обеспечивается организация АРМ с функциями, объединяющими возможности приведенных АРМ. В простейшем случае станционная часть системы может быть реализована на одной ПЭВМ.

Основой периферийной аппаратуры системы являются контроллеры, к которым подключаются считыватели пропусков, СО, кнопки экстренного вызова, отметки наряда, ЭМЗУ, турникеты, внешние устройства, управляемые релейными выходами контроллеров и т.п. Подключение контроллеров к станционной части системы осуществляется с помощью коммуникационных комплектов КР-1, каждый из которых обеспечивает обмен информацией по четырем независимым магистралям длиной до 5 км каждая. Магистраль представляет собой одну витую пару кабеля ТПП или кабеля с аналогичными характеристиками. К каждой магистрали подключается до 25 контроллеров. Программное обеспечение АРМ оператора поддерживает работу до четырех комплектов КР-1, т.е. до 400 контроллеров.

В системе используются контроллеры двух видов:

- К20-07 с функциями контроля доступа и охранной сигнализации,

- К20-11 с функциями охранной сигнализации.

При потере связи с АРМ оператора контроллеры работают автономно, накапливая сообщения в собственном внутреннем архиве. После восстановления связи накопленная в контроллере информация передается на АРМ оператора. Контроллер К20-07 имеет внутреннюю базу данных на 10000 пропусков, используемую в автономном режиме для принятия решения о доступе абонентов.

Система обеспечивает возможность подключения ранее выпускаемых контроллеров К, К-01, К-02 системы "Цирконий-С".

Вместо любого контроллера к магистрали может подключаться терминал или устройство отображения информации "Фокус-СМ", к которому, в свою очередь, подключаются до 16 СО.

Терминал представляет собой многофункциональное устройство, выполняющее в штатном режиме роль пульта управления для установки режимов охраны помещений, а при потере связи с АРМ оператора – роль ведущего устройства, управляющего подключенными к нему контроллерами. Терминал содержит базу данных абонентов, имеющих право установки режимов охраны помещений. Двухуровневая идентификация абонента осуществляется по пропуску и паролю, набираемому на клавиатуре. -



Рисунок 1 – Структурная схема "Цирконий-С2000"

4

При потере связи с АРМ оператора терминал фиксирует поступление тревожного сообщения включением выходного реле (что может быть использовано для передачи на удаленную панель управления) и звукового сигнала. После регистрации пропуска с полномочиями сотрудника службы безопасности на дисплее терминала отображается системный адрес устройства, сформировавшего тревожное сообщение.

Для подключения к магистрали устройства отображения информации "Фокус-СМ" используется специальный адаптер.

Для обеспечения совместной работы с внешними системами: видеонаблюдения, пожарной безопасности, аварийной сигнализации и др., используются стандартные интерфейсы RS-232, RS-485, Ethernet10/100 и соответствующие драйверы.

Программное обеспечение системы, структура которого представлена на рисунке 2, функционирует в среде Windows NT/2000 и включает в себя следующие модули:

|  |  |
| --- | --- |
| Наименование  модуля | Назначение |
| 1 "Конфигуратор" | Конфигурирование системы: состав, связи, режим работы технических средств и их размещение на графических планах. |
| 2 "Администратор" | Ведение базы данных абонентов, операторов рабочих мест, работа с архивом сообщений, формирование и печать отчетов. |
| 3 Оператор" | Обмен информацией с контроллерами, управление периферийной аппаратурой, архив сообщений, взаимодействие с внешними системами: система видеонаблюдения (СВН), СКУД "Сектор-М" и др. |
| 4 "Сеть" | Обмен по сети Ethernet между сервером и АРМ операторов. |
| 5 "РМИП" | Изготовление пропусков на основе Prox-карт, печать учетных карточек о пропусках. |
| 6 "Табельный учет" | Формирование отчетов о состоянии трудовой дисциплины и табелей учета использования рабочего времени. |

В качестве системы управления базами данных (СУБД) используется SQL-сервер (Interвase, Microsoft SQL, Oraсle и др.). Такое решение обеспечивает высокий уровень защищенности информации, хорошие возможности по интеграции системы в автоматизированные системы управления более высокого уровня.

Модульный принцип построения программного обеспечения позволяет создавать АРМ с заданной функциональностью за счет инсталляции соответствующих модулей. Для повышения уровня защиты от несанкционированных действий на каждом АРМ может устанавливаться соответствующий аппаратно-программный комплекс типа "SecretNet".



***Характерные особенности***

* контроль и управление доступом с использованием индивидуального перечня разрешенных зон и графика работы по каждому абоненту;
* поддержка временных и скользящих графиков работы;
* функция antipassback по всей территории объекта, включая нештатные и аварийные ситуации при наличии неконтролируемых связей между зонами объекта (открыта аварийная дверь, точка доступа снята с контроля и т.п.);
* высокая интеграция функций охраны и доступа;
* использование любого сочетания режимов управления охраной помещений:

- автоматического (при входе первого абонента в помещение и вы ходе последнего абонента из помещения);

- централизованного (с АРМ оператора);

- децентрализованного (абонентом с терминала);

* реализация принципа работы по правилу "2"…"6" лиц;
* создание комплексов с малопроводными линиями связи;
* удаление контроллеров от станционной части до 5 км с обеспечением грозозащищенности магистралей;
* дистанционный контроль СО;
* коммутация питания СО;
* широкий диапазон рабочих температур (от минус 50 до плюс 50 оС) для контроллеров с охранными функциями.

***Основные возможности***

**Управление доступом**

Для управления доступом в базу данных абонентов заносятся персональные сведения, включая разрешительные данные, используемые при принятии решения о доступе:

- код пропуска;

- личный код (пароль);

- номера графика работы;

-список зон, разрешенных для посещения;

- тип пропуска (постоянный, временный, разовый);

- период действия временного или разового (обезличенного) пропуска;

-номер временно графика работы;

-период времени временного графика работы.

Временные границы для разрешения доступа определяются номером графика работы. В системе предусмотрено 127 графиков работы. Каждый из них представляет собой годовой календарь, в котором на каждый день проставляется номер смены для рабочего дня или признак выходного, праздничного дня. Номер смены определяет допустимые границы времени входа и пребывания на объекте.

Для абонентов с временными или разовыми пропусками обеспечивается возможность задания права доступа только в присутствии сопровождающего.

После считывания пропуска система идентифицирует абонента, проверяет его разрешительные данные, сравнивает местонахождение считывателя и зону последней регистрации абонента (функция antipassback), проверяет наличие пропуска сопровождающего. При положительных результатах всех проверок доступ абоненту разрешается с уведомлением об этом на индикаторе считывателя, дисплее турникета и т.п.

При отказе в доступе формируется тревожное сообщение на АРМ оператора с указанием причины запрета доступа.

Система поддерживает реализацию алгоритма прохода с видеоверификацией, в этом случае в процедуре идентификации абонента участвует сотрудник службы безопасности (СБ) на АРМ оператора. Решение о доступе принимается по результатам сравнения фото из базы данных абонентов с изображением на мониторе СВН.

По каждому помещению системой может поддерживаться список "вскрывающих"-уполномоченных абонентов, имеющих право входа в пустое помещение, оборудованное на входе средствами контроля и управления доступом, или право управления режимами охраны помещения с терминала. При задании правила "2"…"6" лиц в пустое помещение могут войти только соответственно двое…шесть абонентов из списка "вскрывающих". После этого события в помещение могут входить все допущенные в него абоненты.

Система может поддерживать автоматический режим управления охраной требуемых помещений: при входе первого абонента в помещение снимаются с контроля СО данного помещения, при выходе последнего абонента из помещения – СО берутся на контроль.

Система обеспечивает на всей территории объекта функцию antipassback, контролирующую последовательность проходов абонентом точек доступа на основе сравнения зоны последней регистрации абонента и зоны размещения считывателя, на котором считан пропуск в текущий момент времени.

Наличие функции "antipassback" позволяет системе обнаруживать нарушения режимно-технологической дисциплины (проход через точку доступа без регистрации системой) и попытки проходов по переданному чужому пропуску.

При наличии точек доступа с односторонним контролем (считыватель на входе, кнопка на выходе), а также при нештатных и чрезвычайных ситуациях: снятии точек доступа или аварийных дверей с контроля возникают неконтролируемые связи между зонами объекта. Система в этом случае автоматически учитывает вновь образовавшиеся зоны и сохраняет контроль за последовательностью проходов абонентом через точки доступа. Этим свойством до настоящего времени не обладала ни одна из присутствующих на российском рынке система контроля и управления доступом, оно является уникальным и обеспечивает существенный вклад в повышение уровня безопасности объекта.

***Охранная сигнализация***

Система обеспечивает различные режимы управления охраной зон объекта при подключении СО, датчиков, кнопок экстренного вызова, кнопок отметки наряда и др., имеющих выход в виде нормально-замкнутой или нормально-разомкнутой контактной группы реле.

Система обеспечивает дистанционный контроль СО, имеющих соответствующие цепи управления, в автоматическом режиме до 10 раз в сутки по случайному закону и по командам с АРМ оператора.

Автоматический режим охраны внутренней зоны реализуется при оснащении всех входов в нее средствами контроля и управления доступа, при этом считыватели пропусков устанавливаются с обеих сторон точки доступа. Система автоматически распознает события: вход первого абонента в зону, выход последнего абонента из зоны. При входе первого абонента автоматически в зоне снимаются с контроля СО, которые были указаны для этой цели в процессе конфигурирования системы. При выходе последнего абонента из зоны СО ставятся на контроль. Процедуры снятия с контроля и постановки на контроль могут сопровождаться соответственно отключением и включением питания СО, если это задано при конфигурировании системы и контроллер коммутирует питание только на СО задействованной зоны.

Система обеспечивает охрану протяженных периметров объекта (при использовании контроллеров К20-11, размещаемых в шкафах участковых на периметре) и внутренних зон (при использовании контроллеров К20-07 и К20-11). Контроллер К20-07 позволяет группировать и управлять СО раздельно по 8 зонам.

При централизованном управлении обеспечивается снятие с контроля и постановка на контроль индивидуально каждое СО, каждую зону. При децентрализованном управлении (с терминала) снятие с охраны и постановка на охрану осуществляется только для зоны в целом. При использовании терминалов, работающих в автономном режиме при потере связи с АРМ оператора, снятие с охраны и постановка на охрану возможны только для тех зон, в которых СО управляются контроллерами, подключенными к терминалу.

Терминал опрашивает только те контроллеры, которые физически включены за ним по магистрали.

При поступлении тревожных сообщений АРМ оператора включает звуковой сигнал, отображает графический план объекта с устройством, сформировавшим тревогу, и выдает команды на СВН для коммутации на мониторы соответствующих ситуации телекамер, что позволяет быстро оценить ситуацию и принять адекватные меры.

Функциональные характеристики системы позволяют на ее основе проектировать комплексы охранной сигнализации практически неограниченной емкости, как для защиты периметров, так и внутренних зон объекта.

## Защита информации

Защита информации системы "Цирконий-С2000"от несанкционированного доступа обеспечивается реализацией развитых механизмов контроля и управления, имеющих трехуровневую архитектуру.

Первый уровень защиты, основанный на объединении операторов в различные по своим полномочиям группы, обеспечивается конфигурированием операционной системы АРМ. Большинству операторов предоставляется возможность работы только с модулями системы "Цирконий-С2000".

Второй уровень защиты обеспечивается системой управления базой данных (СУБД), реализованной на SQL сервере. Механизм защиты информации строится на возможности разграничения доступа к информации, хранящейся в таблицах базы данных. При подключении к СУБД проводится обязательная проверка подлинности клиента, после которой ему предоставляются полномочия по просмотру или редактированию данных.

Третий уровень защиты обеспечивается ПО системы. Работа любого оператора в системе "Цирконий-С2000" начинается с идентификации по коду пропуска и личному коду, после чего предоставляются полномочия по управлению системой. Назначение полномочий осуществляется в программном модуле "Администратор" для каждого оператора, и эта работа может быть выполнена только администратором системы. Для каждого оператора назначается список разрешенных для работы программных модулей, а также разрешенные действия, связанные с просмотром и возможностью изменения информации и конфигурирования самой системы.

Помимо решения задач проверки подлинности, определения полномочий и контроля действий, обеспечивается ведение аудита действий операторов системы ‑ информация обо всех действиях оператора сохраняется в архиве сообщений, с указанием сетевого адреса компьютера, времени, объекта действия и команд, подаваемых объекту. Кроме этого в архив сообщений записываются все события, связанные с запуском и остановкой модулей системы. Доступ к архиву сообщений определяется полномочиями оператора.

Показатели защищенности от несанкционированного доступа к информации могут быть улучшены за счет оборудования АРМ дополнительными аппаратно-программными средствами защиты, представленными на рынке.

Помимо защиты информации от несанкционированного доступа, система обеспечивает защиту от сбоев и искажений. Использование серверной СУБД позволяет не только значительно повысить производительность системы, обеспечить разграничение доступа к хранимой информации, но и повысить общую надежность за счет использования таких функций СУБД, как возможность восстановления информации после сбоев, "горячее" резервирование данных, возможность кластерного построения сервера базы данных, создание копии базы данных на внешних носителях.

Таким образом, системой "Цирконий-С2000" обеспечивается высокая степень защиты информации.

***Описание составных частей***

Программное обеспечение

Модуль "Конфигуратор" обеспечивает:

* ведение списка АРМ с указанием сетевых адресов;
* ведение списка зон, контролируемых системой;
* описание аппаратной структуры системы с заданием системных адресов, зон размещения, режимов работы технических средств;
* ведение списка точек доступа с установкой параметров, определяющих алгоритм прохода;
* размещение технических средств на графических планах объекта и формирование иерархии графических планов объекта.

Модуль "Администратор" обеспечивает:

* ведение базы данных абонентов;
* ведение списка операторов системы с заданием полномочий по доступу к информации;
* ведение списков "вскрывающих";
* формирование графиков работы;
* рассылка на АРМ операторов изменений в базе данных абонентов, списке операторов, списках "вскрывающих";
* формирование и печать отчетов о работе системы по архиву сообщений;
* синхронизация времени по всем АРМ;
* создание резервных копий базы данных и архива сообщений за заданный период;

Модуль "Сеть" обеспечивает:

* двухсторонний обмен информацией между сервером и АРМ операторов;
* отображение состояний каналов обмена между сервером и АРМ операторов.

Модуль "Оператор" обеспечивает:

* обмен информацией в реальном времени с контроллерами, терминалами, панелями управления "Фокус-СМ";
* отображение состояния технических средств периферийной аппаратуры;
* меню для подачи команд управления на технические средства;
* регистрацию всех сообщений от периферийной аппаратуры и команд оператора в суточном архиве сообщений;
* рассылку информации о проходах абонентов на другие АРМ операторов для обеспечения функции antipassback;
* автоматический вывод фото абонентов на монитор при проходах через КПП или точки доступа с видеоверификацией;
* автоматический контроль работоспособности технических средств.

Модуль "РМИП" обеспечивает:

* ввод персональных данных абонентов;
* разработку макетов пропусков;
* ввод фото абонентов с использованием цифрового фотоаппарата или сканера;
* печать пропусков на пластиковые Prox-карты с использованием специализированного принтера;
* печать карточек учета выдачи пропусков;
* утверждение в электронном виде изготовленных пропусков для разрешения использования в системе.

Модуль "Табельный учет" обеспечивает:

* формирование и печать за заданный период отчетов по сотрудникам с указанием общего времени работы, времени присутствия в любой из контролируемых зон, опоздания на работу, ухода с работы ранее запланированного времени;
* формирование и печать интегральных показателей состояния трудовой дисциплины (количество опоздавших, количество отсутствующих, количество ушедших раньше с работы) в разрезе подразделений;
* формирование табеля учета использования рабочего времени в соответствии с типовой межотраслевой формой № 13, утвержденной постановлением Госкомстата России;
* экспорт табеля учета использования рабочего времени в текстовый формат с использованием ANSI кодировки.

**Коммуникационный комплект КР-1**

Комплект КР-1 предназначен для:

1. организации магистрали связи между ПЭВМ и контроллерами;
2. контроля состояния блоков питания, подключенных к комплекту КР-1.

Комплект КР-1 состоит из коробки распределительной, размещаемой рядом с ПЭВМ, и субблока ПИ1, устанавливаемого в системный блок.

Комплект КР-1 обеспечивает гальваническую развязку между ПЭВМ и периферийной аппаратурой.

Технические характеристики:

|  |  |
| --- | --- |
| * количество образуемых магистралей, шт. | 4; |
| * длина магистрали, м | 5000; |
| * скорость передачи по магистрали, бит/с | 600/1200/2400; |
| * тип кабеля для магистрали | ТПП; |
| * предельные параметры импульса перенапряжения по шлейфу и цепям питания, наведенного грозовым разрядом: |  |
| * + амплитуда, В | 2000; |
| * + длительность фронта/импульса, мкс | 10/700; |
| * + системная шина ПЭВМ | ISA; |
| * напряжение питания, В | от 20 до 30; |
| * ток потребления, мА | не более 20; |
| * диапазон рабочих температур, °С | от +5 до +40; |
| * габаритные размеры, мм: |  |
| * + субблока ПИ1 | 348х140х22, |
| * + коробки распределительной | 348х210х52; |
| * масса, кг | 2,6 |

**Контроллер К20-07**

Контроллер К20-07 обеспечивает:

- контроль прохода через одну точку доступа;

- контроль состояния шлейфов СО ("обрыв", "короткое замыкание", "норма", "тревога");

- управление ЭМЗУ/турникетом;

- управление внешними устройствами;

- коммутацию питания СО;

- управление по цепям дистанционного контроля СО;

- обмен информацией по магистрали;

- автоматический переход в автономный режим с накоплением информации при пропадании связи с АРМ и автоматическую передачу всех накопленных сообщений на АРМ при восстановлении связи;

- снятие с охраны и постановку на охрану зон.

Контролер К20-07 состоит из блока коммутации и электронного блока, соединяемых через разъем. Это позволяет вести монтаж системы без установки электронных блоков и проводить быстро замену вышедших из строя контроллеров без отключения всей системы.

Технические характеристики:

|  |  |
| --- | --- |
| * напряжение питания, В | от 20 до 30; |
| * ток потребления, мА | не более 100; |
| * количество подключаемых СО, шт. | 5; |
| * количество подключаемых считывателей, шт. | 2; |
| * количество подключаемых ЭМЗУ/турникетов, шт. | 1; |
| * количество подключаемых кнопок, шт. | 2; |
| * количество внешних устройств, шт. | 2; |
| * количество цепей дистанционного контроля, шт. | 2; |
| * расстояние по магистрали от АРМ, м | не более 5000; |
| * коммутируемый ток при подаче питания СО, мА | 300; |
| * коммутируемый ток по цепи управления ВУ   при напряжении ±60 В, А | 1; |
| * диапазон рабочих температур, оС | от плюс 5 до плюс 40; |
| * масса, кг | 2,3. |

**Контроллер К20-11**

Контроллер К20-11 обеспечивает:

- контроль состояния шлейфов СО ("обрыв", "короткое замыкание", "норма", "тревога");

- управление внешними устройствами;

- коммутацию питания СО;

- управление по цепям дистанционного контроля СО;

- обмен информацией по магистрали;

- автоматический переход в автономный режим с накоплением информации при пропадании связи с АРМ и автоматическую передачу всех накопленных сообщений на АРМ при восстановлении связи.

Конструкция контролера К20-11 аналогична конструкции контроллера К20-07.

Технические характеристики:

|  |  |
| --- | --- |
| * напряжение питания, В | от 20 до 30; |
| * ток потребления, мА | не более 100; |
| * количество подключаемых СО, шт. | 10; |
| * количество внешних устройств, шт. | 2; |
| * количество цепей дистанционного контроля, шт. | 2; |
| * расстояние по магистрали от АРМ, м | не более 5000; |
| * коммутируемый ток при подаче питания СО, мА | 300; |
| * коммутируемый ток по цепи управления ВУ   при напряжении ±60 В, А | 1; |
| * диапазон рабочих температур, оС | от минус 50 до плюс 50; |
| * масса, кг | 2,3. |